

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

Four Google, Inc. accounts, more fully described in
Attachment B

Case No. 18-MJ-1279

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment B

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

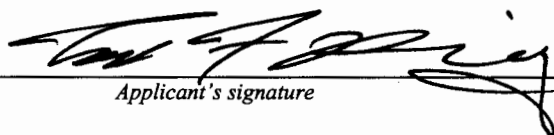
The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 18, United States Code, Sections 1029(a)(2), 1029(a)(3) and 1028A(a)(1)

The application is based on these facts: See attached affidavit.

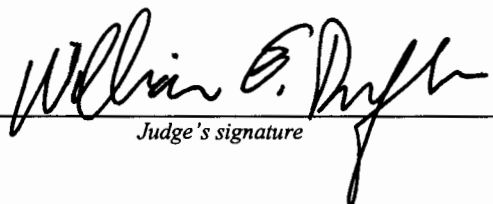
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

Special Agent Todd F. Porinsky, USSS
Printed Name and Title

Sworn to before me and signed in my presence:

Date: 7/12/18


Judge's signature

City and State: Milwaukee, Wisconsin

Honorable William E. Duffin, U.S. Magistrate Judge

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Todd F. Porinsky, Special Agent ("SA") of the United States Secret Service ("USSS"), Cleveland Field Office, (hereinafter referred to as "Affiant"), being first duly sworn, hereby states as follows:

INTRODUCTION

1. Affiant is an investigative or law enforcement officer of the United States within the meaning of Fed. R. Crim. P. 41(a)(2)(C), as a SA of the USSS. Affiant is empowered to conduct investigations of, and to make arrests for, federal offenses pursuant to Title 18, U.S.C. § 3056. Affiant has been employed by the USSS since September 2002, and is assigned to investigate financial crimes in the Criminal Investigative Division. Affiant is responsible for conducting investigations of federal crimes involving identity fraud, credit card fraud, money laundering, bank and wire fraud, and the manufacturing, possession and passing of counterfeit United States currency. At all times during the investigation described in this affidavit, Affiant has acted in an official capacity as a SA of the USSS. Prior to joining the USSS, Affiant was employed as an Infantryman in the United States Marine Corps and an Accounting Technician with the Department of Defense Finance and Accounting Service. In 2017, your affiant was credentialed as a Certified Anti-Money Laundering Specialist.

2. Affiant has participated in all of the usual methods of investigation, including, but not limited to, physical surveillance, the questioning of witnesses, and the analysis of evidence. Affiant has participated in the execution of arrest and search warrants resulting in the seizure of criminally derived property including, but not limited to, monetary instruments.

3. Your Affiant requests a search warrant allowing law enforcement officers to search certain email accounts (Target Email Accounts) held by: Yahoo! (Oath Holdings, Inc.) and Google, Inc., as more fully described below:

Target Email Accounts:

Google, Inc.,

- a. alfeditogouirrie@gmail.com
- b. megacesar2@gmail.com
- c. riveragarcia0610@gmail.com
- d. yunitica@gmail.com

Yahoo! (Oath Holdings, Inc.)

- a. ale_moro2005@yahoo.com
- b. ale_moro2005@yahoo.es
- c. frankabel28@yahoo.com
- d. garciadirian@yahoo.com
- e. gomezsayo@yahoo.com
- f. gomezsayonara@yahoo.com
- g. josuegarcia1990@yahoo.com
- h. maktub631@yahoo.com
- i. richardela@yahoo.com
- j. rivera.sergio32@yahoo.com
- k. yetsycubana@yahoo.es

4. Yahoo! (Oath Holdings, Inc.) is an on-line service provider located in California with a physical address that includes 701 First Avenue, Sunnyvale, CA 94089. This Affiant is requesting www.yahoo.com to disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.

5. Google, Inc. is an on-line service provider located in California with a physical address that includes 1600 Amphitheater Parkway, Mountain View, CA 94043. This Affiant is requesting that www.google.com to disclose the contents of a wire or electronic communication

and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.

6. Such electronic content includes, but is not limited to, contact lists and/or address books, call logs, digital pictures, digital video, digital media, text messages, audio files, e-mails, personal calendars, downloaded Internet content, Internet protocol addresses (IP addresses), GPS points, and records more fully described in Attachment A for Yahoo, Attachment B for Gmail.

7. The statements contained in this affidavit are based in part on information developed by other SAs of the USSS, Federal Bureau of Investigation (FBI), and Officers and Detectives of local police departments in Ohio, Wisconsin, Louisiana, Oklahoma and South Carolina who have aided the investigation. Unless otherwise noted, whenever Affiant asserts that a statement was made, the information was provided by another law enforcement officer or an investigator (with either direct or hearsay knowledge of the statement) with whom Affiant has spoken, or whose report Affiant has read and reviewed. Likewise, any information pertaining to vehicles and registrations, personal data on subjects and record checks, has been obtained through the Law Enforcement Automated Data System (LEADS), various state driver's license motor vehicle records, online database searches, the National Crime Information Center (NCIC) computers, and various open source databases such as Transunion.

8. Since this affidavit is submitted for the limited purpose of supporting the application for a search warrant covering the electronic accounts listed above, Affiant has not included each and every fact known to him concerning this investigation. Affiant has set forth only the facts that which are necessary to establish the probable cause for the issuance of a search warrant for said devices.

9. This Affiant has reason to believe that particular Google, Inc. and Yahoo! account records may contain evidence identifying and linking, victims, suspects, and possible witnesses to the crimes of Title 18, United States Code, Sections 1029(a)(2), 1029(a)(3) and 1028A(a)(1).

10. California Penal Code 1524.2(4)(c) (2006) states that all California Corporations must honor legal process from foreign states when the foreign states are seeking electronic evidence under terms of the Electronic Communications Privacy Act, 18 U.S.C. § 2701 et seq. The Affiant has learned that Google, Inc. is a California Corporation subject to the terms of this California Penal Code 1524.2.

11. This Affiant has learned that Yahoo! is a California Corporation subject to the terms of this California Penal Code 1524.2. Therefore, this Affiant is requesting a search warrant allowing them and/or Law Enforcement Officers to search: Yahoo! (Oath Holdings, Inc.), an on-line service provider located in California with a physical address that includes 701 First Avenue, Sunnyvale, CA 94089, www.yahoo.com to disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record or other information is located within or outside of the United States.

12. The Affiant further requests a search warrant allowing them and/or law enforcement officers to search the phone accounts (Target Phone Accounts) held by: ATT Mobility, T-Mobile, Metro PCS, Consumer Cellular, and Cellco Partnership LLP dba Verizon Wireless, as more fully described below:

Target Phone Accounts:

ATT Mobility
305-915-7228
305-253-2037
305-587-6005

T-Mobile

786-878-2960
786-554-9368
786-972-6898
305-988-3292
786-506-0292
305-699-8792
623-216-8599
623-707-9147
786-856-7039
786-878-0825

Consumer Cellular

305-794-7523

Metro PCS

956-510-2392
786-720-6251
786-857-1600
786-560-6860

Cellco Partnership LLP dba Verizon Wireless

201-280-5622
786-351-7385

13. There is probable cause to believe that the following phone numbers pertaining to ATT Mobility, 11760 US Highway 1, North Palm Beach, FL 33408, are relevant to a legitimate law enforcement inquiry and evidence of the crime, Title 18, United States Code, Sections 1029(a)(2), 1029(a)(3) and 1028A(a)(1):

305-915-7228
305-253-2037
305-587-6005

14. There is probable cause to believe that the following numbers pertaining to T-Mobile, 4 Sylvan Way, Parsippany, NJ 07054, are relevant to a legitimate law enforcement inquiry and evidence of the crime, Title 18, United States Code, Sections 1029(a)(2), 1029(a)(3) and 1028A(a)(1):

786-878-2960
786-554-9368
786-972-6898
305-988-3292
786-506-0292
305-699-8792
623-216-8599
623-707-9147
786-856-7039
786-878-0825

15. There is probable cause to believe that the following phone number pertaining to Consumer Cellular, 12447 SW 69th Ave., Portland, OR 97223, is relevant to a legitimate law enforcement inquiry and evidence of the crime, Title 18, United States Code, Sections 1029(a)(2), 1029(a)(3) and 1028A(a)(1):

305-794-7523

16. There is probable cause to believe that the following phone numbers pertaining to Metro PCS, 2250 Lakeside Blvd, Richardson, TX 75082, are relevant to a legitimate law enforcement inquiry and evidence of the crime, Title 18, United States Code, Sections 1029(a)(2), 1029(a)(3) and 1028A(a)(1):

956-510-2392
786-720-6251
786-857-1600
786-560-6860

17. There is probable cause to believe that the following phone numbers pertaining to Cellco Partnership, LLP dba Verizon Wireless, 180 Washington Valley Rd, Bedminster, NJ 7921, are relevant to a legitimate law enforcement inquiry and evidence of the crime, Title 18, United States Code, Sections 1029(a)(2), 1029(a)(3) and 1028A(a)(1):

201-280-5622
786-351-7385

18. There is probable cause to believe that the following records or other information pertaining to the business transactions of ATT Mobility, T-Mobile, Consumer Cellular, Metro PCS and Celco Partnership, LLP dba Verizon Wireless are relevant to a legitimate law enforcement inquiry and evidence of the crime, Title 18, United States Code, Sections 1029(a)(2), 1029(a)(3) and 1028A(a)(1).

19. All customer/subscriber information, including any listed addresses, telephone numbers, social security numbers, dates of birth, names, addresses, any other customer identifying information, mobile handset or device identifiers/serial numbers (MEID, ESN, IMSI, IMEI), activation date and deactivation date, and location device was purchased if applicable.

20. Device Purchase Information. This is specifically to include the Date, Time and Location of where the device or any pre-paid refill cards were purchased.

21. Any email addresses associated with the account. This is to specifically include Google Gmail addresses associated with any Android device associated with this device or any email associated with an iPhone and/or iTunes account associated with this device that is currently on file and stored in the normal course of business of the cellular service provider.

22. Call detail records, including detailed information in reference to all known outgoing and incoming calls associated with the account, dates and times calls were made, and duration of all calls made or received. This is to include any other pertinent call detail records including special features codes, or any other codes that are maintained in the normal course of business for the cellular service provider, of any cellular numbers identified in the course of the investigation. In addition to voice calls, this would also include any detail records showing text messages, MMS messages, or data activity.

23. In the event the requested Call Detail Records contain other cellular service provider customer numbers, identified as either incoming or outgoing calls, the cellular service provider will provide subscriber information to the specific numbers identified, if requested.

24. Cell site information, to include all known cell towers associated with outgoing and incoming calls (Call Detail Records). This information is to include any sector information, if known, cell site location, and any other related material that would be necessary to identify the location and sector in reference to the cell site information associated with the call detail records. In the event text messages, MMS messages, LTE and Data activity including IP session and destination addresses that were produced are also available with cell site information, this information would be included in this request.

25. Cell Site locations for all cellular service provider Cell Sites, sector information, including Azimuth headings, in the regional market associated with the requested cell site information.

26. Location information, to include any estimated or known Longitude and Latitude of the cellular device's current location, or approximate location, and information received by cell tower(s) in reference to direction and distance from the tower a device may be located (timing and triangulation information). Radio Frequency signal strengths, direction, and transmission information. The geographical constraints of location information will be limited to the United States.

27. Location information can be in the form of historical records. Specific to ATT Mobility, this would include any reports of device activity that would include the approximate latitude and longitude of the device at the time of the activity, direction and distance from the

tower, and other location related information commonly referred to as a NELOS report. This further includes any other report similar in nature.

28. Specific to T-Mobile, historical records of location information would include any reports of device activity that would include the approximate latitude and longitude of the device at the time of the activity, direction and distance from the tower, and other location related information commonly referred to as a TrueCall report. This further includes any other report similar in nature. For real-time location information this would include the E-911 automated email system, providing emails to the affiant every 15 minutes with the estimated latitude and longitude of the device. For real-time location information this would include the E-911 automated email system, providing emails to the affiant every 15 minutes with the estimated latitude and longitude of the device.

29. Specific to Consumer Cellular, historical records of location information would include any reports of device activity that would include the approximate latitude and longitude of the device at the time of the activity, direction and distance from the tower, and other location related information commonly referred to as a PCMD, RTT or RTD report. This further includes any other report similar in nature. For real-time location information this would include the E-911 automated email system, providing emails to the affiant every 15 minutes with the estimated latitude and longitude of the device.

30. Specific to Metro PCS, historical records of location information would include any reports of device activity that would include the approximate latitude and longitude of the device at the time of the activity, direction and distance from the tower, and other location related information, commonly referred to as a TrueCall report. This further includes any other report similar in nature. For real-time location information this would include the E-911 automated email

system, providing emails to the affiant every 15 minutes with the estimated latitude and longitude of the device.

31. Specific to Cellco Partnership, LLP dba Verizon Wireless, historical records of location information would include any reports of device activity that would include the approximate latitude and longitude of the device at the time of the activity, direction and distance from the tower, and other location related information commonly referred to as an RTT, EVDO, ALULTE, and Levdot report. This further includes any other report similar in nature. For real-time location information this would include the E-911 automated email system, providing emails to the affiant every 15 minutes with the estimated latitude and longitude of the device.

32. All text message and/or MMS messages currently stored in the normal course of business for ATT Mobility, to include any cloud services which allow for the long term storage of both voicemails and SMS/MMS messages.

33. For ATT Mobility, it is requested that the above records be provided in both of AT&T's Text(.txt) and PDF(.pdf) formats.

34. The above information is being requested for unknown subscribers in reference to the following mobile devices:

- a. Telephone: 305-915-7228
305-253-2037
305-587-6005
Service Provider: ATT Mobility
Location: 11760 US Highway 1, North Palm Beach, FL 33408
- b. Telephone: 786-878-2960
786-554-9368
786-972-6898
305-988-3292
786-506-0292
305-699-8792
623-216-8599
623-707-9147

786-856-7039

786-878-0825

Service Provider: T-Mobile

Location: 4 Sylvan Way, Parsippany, NJ 07054

c. Telephone: 305-794-7523

Service Provider: Consumer Cellular

Location: 12447 SW 69th Ave., Portland, OR 97223

d. Telephone: 956-510-2392

786-720-6251

786-857-1600

786-560-6860

Service Provider: Metro PCS

Location: 2250 Lakeside Blvd, Richardson, TX 75082

e. Telephone 201-280-5622

786-351-7385

Service Provider: Cellco Partnership, LLP dba Verizon Wireless

Location: 180 Washington Valley Rd, Bedminster, NJ 7921

35. The information described above for ATT Mobility, T-Mobile, Consumer Cellular, Metro PCS and Cellco Partnership, LLP dba Verizon Wireless is being requested during the following time period:

a. Historical Records – March 1, 2016 to July 12, 2018

b. Real Time/Provisional Records – July 13, 2018 to July 27, 2018.

36. The specific records more fully described in Attachment C for ATT Mobility, Attachment D for T-Mobile, Attachment E for Metro PCS, Attachment F for Consumer Cellular, and attachment G for Cellco Partnership LLP dba Verizon Wireless.

BACKGROUND: CELLULAR TELEPHONES AND ELECTRONIC DEVICES

37. Through Affiant's training and experience, Affiant is aware of the following:

a. Cellular Telephones: Cellular telephones allow users to connect to other users of cellular telephones through voice, email, and text messaging.

b. Cellular telephones have the capability of using GPS to display their current locations. A cellular telephone, when functioning as a GPS navigation device, often records the locations where it has been.

c. Cellular telephones have the capability to connect to the Internet through “Wi-Fi” or a cellular telephone carrier’s network. An IP address is a unique numeric address used by devices on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). An IP address allows Internet traffic to be directed properly from its source to its destination.

d. Cellular telephones have the capability to download digital pictures, digital video, digital media, and audio files.

e. Cellular telephones often store contact lists or “address books” and personal calendars for users.

f. Individuals involved in criminal activity use cellular telephones to facilitate crimes. Specifically, Affiant is aware that individuals involved in criminal activity use cellular telephones, whether through telephone conversations, email, or text messages, as a medium to communicate with co-conspirators during the planning and commission of crimes.

g. Those involved in criminal activity frequently keep names, email addresses and phone numbers of co-conspirators in the electronic contact list or address book utility located within the cellular telephone device.

h. Individuals involved in criminal activity will frequently disconnect the battery from their cellular telephone in attempts to avoid detection by law enforcement.

i. A cellular telephone can be used to store data and play audio, video, or photographic files. These digital files can be transmitted electronically via email communications. The record of these email communications can be maintained in the cellular telephone memory, or maintained remotely at the email provider facilities.

j. Skimmers: One type of electronic device that attaches to the computer of the point-of-sale credit card reader is commonly referred to as a skimmer. They are often found illicitly placed on gas station pumps. The device copies the electronically transmitted full track data found on the magnetic strip of a customer's credit card, to enable valid electronic payment authorization to occur between a merchant and the issuing financial institution. The credit card data is fraudulently accumulated and stored on the skimmer to be later removed or transmitted to a computer directly or through a Wi-Fi connection. Once connected to a computer, the skimmer has the ability to transfer the digital content (i.e., the fraudulently obtained credit card data) to a personal computer.

k. Credit card reader/writer/encoder: Credit Card reader/writers are designed to provide a means to read and re-write the data found on the magnetic strips of credit cards. They have the ability to read and write tracks 1, 2, and 3 of data, while simultaneously decoding, encoding, and verifying three tracks of data. Examples of cards that can be read and re-written include credit cards, loyalty cards, gift cards, employee ID cards and hotel room keys. The three tracks can contain some combination of the following: Track 1 and/or Track 2 typically have Primary Account No. (19 digits Max.), Account Name (26 alphanumeric characters Max.), Expiration date (YYMM), Service Code and Discretionary Data. Track 3 can have Primary Account No., Country Code (optional), Currency Code, Currency Exponent, Amount Authorized per Cycle, Amount

Remaining this Cycle, Cycle Begin (Validity Date), Cycle Length, Retry Count, PIN Control Parameters (optional), Interchange Controls, PAN Service Restriction, SAN-1 Service Restriction, SAN-2 Service Restriction, Expiration Date (optional), Card Sequence Number, Card Security Number (optional), First Subsidiary Account No., (optional), Secondary Subsidiary Account No. (optional), Relay Marker, and/or Cryptographic Check Digits (optional). These devices are frequently used by individuals to encode stolen credit card data onto blank or counterfeit plastic credit card, gift cards or blank "white plastic" cards.

1. Credit card reader: Credit card readers are similar to a credit card reader/writer/encoder, but can only read the data from the magnetic strip of a credit card or similar card. It cannot write or encode data to the magnetic strip of a card. When attached to a computer, the card reader enables the user to view and store stolen data from the cards scanned on the computer.

m. Laptop: A laptop is a mobile computer, typically the size of a notebook, which is mobile, battery operated and easily transported. Laptops can function as wireless communication devices and can be used to access the Internet through cellular networks, Wi-Fi networks, or otherwise. Laptops typically contain programs, the same as a personal computer, which perform different functions and save data associated with those functions. Programs can, for example, enable accessing of the Internet, sending and receiving email, and participating in Internet social networks.

n. An Inspiron 15 is a laptop manufactured by Dell. A Dell Inspiron 15 has the capability to connect to the Internet through Wi-Fi or a cellular telephone carrier's network. Once connected to the Internet, a Dell Inspiron 15 has the capability to download

digital pictures, digital video, digital media, and audio files. A Dell Inspiron 15 also has the capability to function as a "blue tooth device," through the use of its ability to receive and transmit data wirelessly through a wireless "blue tooth" program and transmitter/receiver.

o. Removable storage media: Laptops, skimmers, and other electronic devices often have the capability to connect to removable storage media that store electronic data. Removable storage media include various types of flash memory cards and miniature hard drives. This type of removable storage media can store any type of digital data. Such data can be obtained by connecting the removable storage media directly to a computer or by connecting the removable storage media to a separate reader.

p. Cellular Phones: Cellular phones, such as variations of the iPhone Model 5, iPhone Model 6 and iPhone Model 7, have the capability of communicating via voice calls, text messages and email.

q. Examining data stored on devices of the types described above can uncover, among other things, evidence that reveals or suggests who possessed or used the device. Investigators can identify with whom a device was used to communicate through analytics performed on data such as, and not limited to, the device's call logs, contact lists, device event history, SMS and MMS text records, IP locations, and through GPS locations/time stamps on shared files.

38. Based on Affiant's knowledge, training, and experience, Affiant knows that email providers, such as Google, Inc. and Yahoo! can store information for long periods of time. Similarly, data, information or websites that have been viewed on the Internet are typically stored

for some period of time by these email providers. This information can sometimes be recovered and provided to authorities pursuant to a court order.

BACKGROUND: HISTORICAL GOOGLE ACCOUNT RECORDS

39. Based on this Affiant's prior training and experience and after reviewing Google, Inc.'s privacy statement, this Affiant is aware that users of Google Gmail and Google services and which this Affiant seeks a search warrant for, commonly have an associated account with Google, Inc. When a user purchases and activates a mobile device one of the initial prompts during the set-up phase is to associate a Google Gmail account with the device. The purposes of this account are to facilitate a password reset in the event the consumer forgets their passcode, pattern unlock, or password. If the consumer does not have an existing Gmail account, the operating system prompts the user to create a new account. Whether the Gmail account is new or existing the association of the account with the device allows Google to collect and store information relevant to this criminal investigation. This information includes, by way of example and not limitation:

- a. Account Information - User name, primary email address, secondary email addresses, connected applications and sites, and account activity since March 1, 2016, including account sign in locations, browser information, platform information, and internet protocol (IP) addresses. Google maintains information about their customers including primary email addresses, secondary email addresses for account password recovery, applications, websites, and services that are allowed to access the user's Google account or use the user's Google account as a password login, and account login activity such as the geographic area the user logged into the account, what type of internet browser and device they were using, and the internet protocol (IP) address they logged in from. The IP address is roughly analogous to a telephone number assigned to a

computer by an internet service provider. The IP can be resolved back to a physical address such as a residence or business with Wi-Fi access or residential cable internet. This Affiant believes this information will assist in the investigation by identifying previously unknown email accounts and location history information tending to show the movements of the suspect, his mobile device, and/or computers;

b. Android Information - Device make, model, and International Mobile Equipment Identifier (IMEI) of all associated devices linked to the Google accounts of the target account. Google stores information about mobile devices associated with the user's Google account. This includes the make, model, and unique serial numbers of all linked devices. This Affiant believes this information will identify any previously unknown cell phones or other mobile devices associated with the suspect's account and/or known device(s);

c. User attribution data – accounts, e-mail accounts, passwords, PIN codes, account names, user names, screen names, remote data storage accounts, credit card number or other payment methods, contact lists, calendar entries, text messages, voice mail messages, pictures, videos, telephone numbers, mobile devices, physical addresses, historical GPS locations, two-step verification information, or any other data that may demonstrate attribution to a particular user or users of the account(s).

This Affiant knows that Google may not verify the true identity of an account creator, account user or any other person who accesses a user's account using login credentials. For these reasons it is necessary to examine particularly unique identifying information that can be used to attribute the account data to a certain user. This is often accomplished by analyzing associated account data, usage, and activity through communication,

connected devices, locations, associates, and other accounts. For these reasons it may be necessary to search and analyze data from when the Google account was initially created to the most current activity;

- d. Calendar - All calendars, including shared calendars and the identities of those with whom they are shared, calendar entries, notes, alerts, invites, and invitees.

Google offers a calendar feature that allows users to schedule events. This calendar function is the default option in the Android operating system and remains so unless the user adds a third party application. Calendar events may include dates, times, notes and descriptions, others invited to the event, and invitations to events from others. This Affiant believes this information will identify dates and appointments relevant to this investigation, as well as, identify previously unknown co-conspirators and/or witnesses, and any potential corroborative evidence;

- e. Contacts - All contacts stored by Google including name, all contact phone numbers, emails, social network links, and images. When a user links the Android device to their Google account the names, addresses, phone numbers, email addresses, notes, and pictures associated with the account are transferred to the phone and vice versa. This process continuously updates so when a contact is added, deleted, or modified using either the Google account or the mobile device the other is simultaneously updated. This Affiant believes this information is pertinent to the investigation as it will assist with identifying previously unknown coconspirators and/or witnesses.

- f. Docs (Documents) - All Google documents including by way of example and not limitation, Docs (a web based word processing application), Sheets (a web-based

spreadsheet program), and Slides (a web based presentation program.) Documents will include all files whether created, shared, or downloaded.

g. Documents - All user created documents stored by Google; Google offers their users access to free, web-based alternatives to existing word processing, spreadsheet, and presentation software. These documents are stored in the user's account and are accessible from any device or platform as long as the user knows the password. These documents can include those created by the user, modified or edited by the user, or shared by the user and others. This Affiant believes this information may contain notes, files, and spreadsheets containing information relevant to this investigation including recordation of sales, communications with unknown co-conspirators and/or witnesses, and other information concerning the ongoing investigation;

h. Finance - All records of securities, funds, and portfolios associated with the target Google account and/or target device. Google allows users to create custom portfolios of stocks, bonds, and mutual funds. These portfolios are updated based on the market conditions and contain the investment type and the dollar value of the investment. This Affiant believes this data may contain information about income, investments, and previously undiscovered assets derived as proceeds from the ongoing criminal enterprise;

i. Gmail - All email messages, including by way of example and not limitation, such as inbox messages whether read or unread, sent mail, saved drafts, chat histories, and emails in the trash folder. Such messages will include all information such as the date, time, internet protocol (IP) address routing information, sender, receiver, subject line, any other parties sent the same electronic mail through the 'cc' (carbon copy) or the 'bcc' (blind carbon copy), the message content or body, and all attached files.

As noted previously, when user of an Android device first activates the device they are prompted to associate the device with a Google mail, commonly referred to as Gmail, account. The purpose of this account is to facilitate password recovery in the event the user forgets their password or pattern lock. If the user does not have an existing Gmail account, they are prompted to create one. The Gmail account may be used to send and receive electronic mail messages and chat histories. These messages include incoming mail, sent mail, and draft messages. Messages deleted from Gmail are not actually deleted. They are moved to a folder labelled Trash and are stored there until the user empties the Trash file. Additionally, users can send and receive files as attachments. These files may include documents, videos, and other media files. This Affiant believes these messages would reveal motivations, plans and intentions, associates, and other co-conspirators;

j. Google Photos - All images, graphic files, video files, and other media files stored in the Google Photos service. Google users have the option to store, upload, and share digital images, graphic files, video files, and other media files. These images may be downloaded from the internet, sent from other users, or uploaded from the user's mobile device. In many cases, an Android user may configure their device to automatically upload pictures taken with a mobile device to their Google account. This Affiant believes a review of these images would provide evidence depicting the suspect, his/her associates and others performing incriminating acts, and victims. This Affiant also believes these image files may assist investigators with determining geographic locations such as residences, businesses, and other places relevant to the ongoing criminal investigation;

k. Location History - All location data whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, precision measurement information such as timing advance or per call measurement data, and Wi-Fi location. Such data shall include the GPS coordinates and the dates and times of all location recordings from the period March 1, 2016 to the present.

Google collects and retains location data from Android enabled mobile devices. The company uses this information for location based advertising and location based search results. Per Google, this information is derived from Global Position System (GPS) data, cell site/cell tower information, and Wi-Fi access points. While the specific parameters of when this data is collected are not entirely clear, it appears that Google collects this data whenever one of their services is activated and/or whenever there is an event on the mobile device such as a phone call, text messages, internet access, or email access. This Affiant believes this data will show the movements of a suspect's mobile device and assist investigators with establishing patterns of movement, identifying residences, work locations, and other areas that may contain further evidence relevant to the ongoing criminal investigation;

l. Play Store - All applications downloaded, installed, and/or purchased by the associated account and/or device. Google operates an online marketplace whereby Google and other third party vendors offer for sale applications such as games, productivity tools, and social media portals. Many of these applications can be used to communicate outside the cellular service of a mobile device by accessing the internet via Wi-Fi.

These various applications facilitate communication via voice using voice over internet protocol (VOIP) technology, short message system (SMS) text messages, multi-

media message system (MMS) text messages, audio transmission of recorded messages, and recorded or live video messages. As these services operate independently of the cellular service network there is no corresponding information regarding communications from the cellular provider. Identifying communications applications purchased, downloaded, and/or installed on the mobile device would assist investigators by determining what application provider should be served with additional search warrants. Furthermore, identifying the user's applications would assist investigators with determining banking and other financial institution information and social media sites used. Identifying the purchased or installed applications would assist locating those with potentially criminal implications such as applications that appear to the observer to be a calculator or other innocuous appearing program but in actuality are used to conceal pictures, videos, and other files. These concealment applications are commonly missed during manual and forensic examinations of mobile devices as existing technologies are not designed to detect and locate them and the information they conceal;

- m. Search History - All search history and queries, including by way of example and not limitation, such as World Wide Web (web), images, news, shopping, ads, videos, maps, travel, and finance. Google retains a user's search history whether it is done from a mobile device or from a traditional computer. This history includes the searched for terms, the date and time of the search, and the user selected results. Furthermore, these searches are differentiated by the specific type of search a user performed into categories. These categories include a general web search, and specialty searches where the results are focused in a particular group such as images, news, videos, and shopping. This Affiant believes a review of a suspect's search history would reveal information relevant

to the ongoing criminal investigation by revealing what information a suspect sought and when he sought it;

n. Voice - All call detail records, connection records, short message system (SMS) or multimedia message system (MMS) messages, and voicemail messages sent by or from the Google Voice account associated with the target account/device; Google offers users access to a free voice over internet protocol (VOIP) communications system called Google Voice or simply Voice. This system is layered on top of any existing cellular service. Users are provided with a phone number they select from a pool of available numbers. These numbers can be from whatever area code and prefix they desire and have no correlation with the user's actual location when the number is selected. Google allows users to access this system to make and receive phone calls and text messages. The service also has a voicemail feature where incoming phone calls are permitted to leave a message that is subsequently transcribed by Google and delivered by electronic mail and/or text message. Google maintains call detail records similar to those of a traditional cellular or wireline telephone company. Additionally, they also store the text message content of sent and received text messages, as well as any saved voicemail messages and the associated transcriptions.

o. Wallet/Checkout - All information contained in the associated Google Wallet account including transactions, purchases, money transfers, payment methods, including the full credit card number and/or bank account numbers used for the transactions, and address book. Google operates a financial services division that allows users to make online purchases through Google and other vendors, as well as, send and receive money from other users. Applications that are purchased and installed on a mobile device are

handled by Google's Wallet/Checkout service. The purchase and installation of applications on a mobile device requires the use of the Google Wallet service. Therefore, any applications installed on the suspect's mobile phone have a transaction record in Google Wallet. Google stores information regarding the transactions including the date and time of the purchase. Additionally, they have method of payment information such as associated credit card numbers used to facilitate the purchase. Other data includes the billing address of any linked credit card and any addresses where purchased products were shipped to. This Affiant believes that identifying the method of payment information would assist investigators with identifying any previously unknown financial institutions and that these financial institutions may have additional relevant information pertinent to this investigation.

- p. Google Home (Smart Speaker & Home Assistant) - All information related to Google Home including device names, serial numbers, Wi-Fi networks, addresses, media services, linked devices, video services, voice and audio activity, and voice recordings with dates and times. Google Home is a brand of smart speaker developed by Google, Inc. Google Home Speakers have microphones that are always listening that enable users to speak voice commands to interact with services through Google's intelligent personal assistant called Google Assistant. A large number of services, both in-house and third-party, are integrated, allowing users to listen to music, control playback of videos and photos, and receive news updates entirely by voice. Google Home devices also have integrated support for home automation, letting users control smart home appliances with their voice. Multiple Google Home devices can be placed in different rooms in a home for synchronized connectivity. The data collected by Google Home devices are stored

remotely on Google's servers. Users can access their Google Home account and associated data by way of a connected smart phone application or through their Google account. This Affiant believes that Google Home related data, including archived audio recordings, may be used to refute and corroborate statements, and may be important in identifying potential witnesses, victims, co-conspirators, and suspects. This information may also be important in establishing a timeline and provide context and intent.

q. Android Auto - All information related to Android Auto including device names, serial numbers and identification numbers, device names, maps and map data, communications including call logs and text messages, voice actions, and all location data. Android Auto is a mobile device application developed by Google that allows enhanced use of an Android device within a vehicle equipped with a compatible head unit. Once the Android device is connected to the head unit, the system enables it to broadcast applications (apps) with a simple, driver-friendly user interface onto the vehicle's dash display, including GPS mapping/navigation, music playback, text messages (SMS), voice calls, and web search. The system supports both touchscreen and button-controlled head unit displays, although hands-free operation through voice commands is encouraged. Once the user's Android device is connected to the vehicle, the Android mobile device will have access to several of the vehicle's sensors and inputs, such as GPS, steering-wheel mounted buttons, the sound system, directional microphones, wheel speed, compass, and other vehicle data.

40. For the reasons that follow, this Affiant believes probable cause exists to seize and examine the specified records held by Google, Inc. associated with the accounts

alfeditogouirrie@gmail.com, megacesar2@gmail.com, riveragarcia0610@gmail.com and yunitica@gmail.com.

BACKGROUND: HISTORICAL YAHOO! ACCOUNT RECORDS

41. Yahoo! maintains information about their customers including primary email addresses, secondary email addresses for account password recovery, applications, websites, and services that are allowed to access the user's Yahoo! account or use the user's Yahoo! account as a password login, and account login activity such as the geographic area the user logged into the account, what type of internet browser and device they were using, and the internet protocol (IP) address used to log in. The IP address is roughly analogous to a telephone number assigned to a computer by an internet service provider. The IP can be resolved back to a physical address such as a residence or business with Wi-Fi access or residential cable internet. This Affiant believes this information will assist in the investigation by identifying previously unknown email accounts and location history information tending to show the movements of a suspect, his/her mobile device, and/or computers.

42. This Affiant knows that Yahoo! (Oath Holdings, Inc.) may not verify the true identity of an account creator, account user or any other person who accesses a user's account using login credentials. For these reasons it is necessary to examine particularly unique identifying information that can be used to attribute the account data to a certain user. This is often accomplished by analyzing associated account data, usage, and activity through communication, connected devices, locations, associates, and other accounts. For these reasons it may be necessary to search and analyze data from when the Yahoo! account was initially created to the most current activity. This information includes, by way of example and not limitation:

- a. Calendar - All calendars, including shared calendars and the identities of those with whom they are shared, calendar entries, notes, alerts, invites, and invitees. Yahoo! offers a calendar feature that allows users to schedule events. Calendar events may include dates, times, notes and descriptions, others invited to the event, and invitations to events from others. This Affiant believes this information will identify dates and appointments relevant to this investigation, as well as, identify previously unknown co-conspirators and/or witnesses, and any potential corroborative evidence.
- b. Contacts - All contacts stored by Yahoo! (Oath Holdings, Inc.) including name, all contact phone numbers, emails, social network links, and images. When a user links to their Yahoo! using a tablet or mobile device, the names, addresses, phone numbers, email addresses, notes, and pictures associated with the account may be transferred to the mobile device and vice versa. This process may continuously update so when a contact is added, deleted, or modified using either the Yahoo! account or the mobile device the other is simultaneously updated. This Affiant believes this information is pertinent to the investigation as it will assist with identifying previously unknown coconspirators and/or witnesses.
- c. Docs (Documents) - All documents including by way of example and not limitation, Docs (a web based word processing application), Sheets (a web-based spreadsheet program), and Slides (a web based presentation program.) Documents will include all files whether created, shared, or downloaded.
- d. Yahoo! Mail - All email messages, including by way of example and not limitation, such as inbox messages whether read or unread, sent mail, saved drafts, chat histories, and emails in the trash folder. Such messages will include all information such as the

date, time, internet protocol (IP) address routing information, sender, receiver, subject line, any other parties sent the same electronic mail through the 'cc' (carbon copy) or the 'bcc' (blind carbon copy), the message content or body, and all attached files. The Yahoo! account may be used to send and receive electronic mail messages and chat histories. These messages include incoming mail, sent mail, and draft messages. Messages deleted from Yahoo! are not actually deleted. They are moved to a folder labelled Trash and are stored there until the user empties the Trash file. Additionally, users can send and receive files as attachments. These files may include documents, videos, and other media files. This Affiant believes these messages will reveal motivations, plans and intentions, associates, and other co-conspirators.

- e. Photos -All images, graphic files, video files, and other media files stored by Yahoo! for the listed account. Yahoo! users may have the option to store, upload, and share digital images, graphic files, video files, and other media files. These images may be downloaded from the Internet, sent from other users, or uploaded from the user's mobile device. This Affiant believes a review of these images would provide evidence depicting a suspect, his/her associates and others performing incriminating acts, and victims. This Affiant also believes these image files may assist investigators with determining geographic locations such as residences, businesses, and other places relevant to the ongoing criminal investigation.
- f. Location History - All location data whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, precision measurement information such as timing advance or per call measurement data, and Wi-Fi location. Such data shall include the GPS coordinates and the dates and times of all

location recordings from the period March 1, 2016 to the present. Yahoo! may collect and retain location data from user mobile devices. The company may use this information for location based advertising and location based search results. While the specific parameters of when this data is collected are not entirely clear, it appears that Yahoo! collects this data whenever one of their services is activated and/or whenever there is an event on the mobile device. This Affiant believes this data will show the movements of a suspect's mobile device and assist investigators with establishing patterns of movement, identifying residences, work locations, and other areas that may contain further evidence relevant to the ongoing criminal investigation.

g. Search History - All search history and queries, including by way of example and not limitation, such as World Wide Web (web), images, news, shopping, ads, videos, maps, travel, and finance. Yahoo! retains a user's search history whether it is done from a mobile device or from a traditional computer. This history includes the searched for terms, the date and time of the search, and the user selected results. Furthermore, these searches are differentiated by the specific type of search a user performed into categories. These categories include a general web search, and specialty searches where the results are focused in a particular group such as images, news, videos, and shopping. This Affiant believes a review of a suspect's search history would reveal information relevant to the ongoing criminal investigation by revealing what information the suspect sought and when he or she sought it.

43. For reasons that follow, this Affiant believes probable cause exists to seize and examine the specified records held by Yahoo! associated with the accounts ale_moro2005@yahoo.com, ale_moro2005@yahoo.es, frankabel28@yahoo.com,

garciadirian@yahoo.com, gomezsayo@yahoo.com, gomezsayonara@yahoo.com,
josuegarcia1990@yahoo.com, maktub631@yahoo.com, richardela@yahoo.com,
rivera.sergio32@yahoo.com and yetsycubana@yahoo.es.

Evidence to be Searched and Seized

44. This application seeks permission to search for and seize evidence of violations of Title 18, United States Code, Sections 1029(a)(2), 1029(a)(3) and 1028A(a)(1), described in Attachment A and Attachment B, that are associated with records currently under the control of Google, Inc. or Yahoo! (Oath Holdings, Inc.). The specific Google accounts are associated with the email addresses named alfeditogourrie@gmail.com, megacesar2@gmail.com, riveragarcia0610@gmail.com and yunitica@gmail.com. The specific Yahoo! accounts are associated with the email names ale_moro2005@yahoo.com, ale_moro2005@yahoo.es, frankabel28@yahoo.com, garciadirian@yahoo.com, gomezsayo@yahoo.com, gomezsayonara@yahoo.com, josuegarcia1990@yahoo.com, maktub631@yahoo.com, richardela@yahoo.com, rivera.sergio32@yahoo.com and yetsycubana@yahoo.es. Further, this application seeks permission to search for and seize evidence of violations of Title 18, United States Code, Sections 1029(a)(2), 1029(a)(3) and 1028A(a)(1), described in Attachment C ATT Mobility for accounts 305-915-7228, 305-253-2037, 305-587-6005; Attachment D T-Mobile for accounts 786-878-2960, 786-554-9368, 786-972-6898, 305-988-3292, 786-506-0292, 305-699-8792, 623-216-8599, 623-707-9147, 786-856-7039, 786-878-0825; Attachment E Consumer Cellular for account 305-794-7523; Attachment F Metro PCS for accounts 956-510-2392, 786-720-6251, 786-857-1600, 786-560-6860; and Attachment G Cellco Partnership LLP dba Verizon Wireless for accounts 201-280-5622, 786-351-7385.

FACTUAL BACKGROUND

45. Agents and analysts assigned to USSS Cleveland Field Office, Milwaukee Field Office, Miami Field Office, Investigative Support Division and other offices have conducted an investigation beginning in December 2016, which has included suspect and witness interviews, review of financial records, review of phone records, and forensic analysis of suspects' computers and cell phone data. The incidents described below constitute a multi-state identity theft and money laundering conspiracy. The co-conspirators worked in various roles in a combined effort to steal credit card information from gas pump customers using data recorders known as skimmers. Those credit card numbers were then encoded onto counterfeit credit cards. These counterfeit cards were then used to buy "clean" retail gift cards and merchandise.

46. Specifically, Richard Rivera Garcia is known to have worked in a criminal organization with, made payments to, and/or given direction to the following individuals, who are known to have travelled across the United States to participate in the theft of victim credit card data, production of counterfeit cards, shopping with counterfeit credit cards or acting as drivers for others participating in such activities:

Josue Moret of Miami, FL; Walter Enrique Estrada of Peoria, AZ; Gabriel Delgado Ramirez of Miami, FL; Alejandro Luis Dewelde of Opa Locka, FL; Geosvany Gonzalez Valdez of Tampa, FL; Frank Abel Bernal of Hialeah, FL; Juan Zabala of Phoenix, AZ; Nilo Nunez Perez of Miami, FL; Alejandro Rodriguez Martinez of Miami, FL; Jose Javier Moreiras of Miami, FL; Lorenzo F. Hernandez of Miami, FL; Cesar David Lopez of Hialeah, FL; Alfredo Gouirrie Blanco of Cape Coral, FL.

47. Additionally, Inlian Sayonara Gomez of Miami, FL, is known to have recorded the group's purchases of gift cards as they travelled across the country. She communicated this informal bookkeeping to Rivera Garcia via cell phone text messages and photographs.

Greendale Police Department Investigation

48. On March 29, 2016, a man (later identified as Walter Enrique Estrada) used fraudulent credit cards to purchase \$350.00 worth of Kohl's gift cards and \$300.00 worth of Best Buy gift cards from the Kohl's store located at 5300 S. 76th St., in Greendale, Wisconsin. On April 14, 2016, a man (later identified as Estrada) used a fraudulent Visa credit card and a fraudulent MasterCard to purchase two \$300.00 gift cards from the Kohl's store. In both instances, Greendale Police Officers Robert Utech, Michael Adamczak and Detective Julie Barth spoke to the Kohl's loss prevention officer and interviewed victims to establish the gift card purchases were not authorized by the card holders. Later review of store video from those dates shows the person appearing on the videos matched the appearance of Estrada making the purchases at Kohl's.

49. On April 15, 2016, in the Greendale Kohl's store, a Kohl's loss prevention officer recognized the man who had used the fraudulent credit cards the previous day. The man used several different credit cards that were declined while attempting to purchase a suitcase, cologne and two gift cards for \$300 each. Eventually, a credit card was used and the transaction was approved. The loss prevention officer described the man's outfit and a vehicle description of a black Nissan Altima with New York license plates to the Greendale Police via radio. Greendale Police Detective Barth observed the man exit the Kohl's store and walk to a black Nissan Altima in the parking lot and enter the passenger seat. Officer Barth and other officers followed the black Nissan Altima. The officers conducted a vehicle stop after the black Nissan appeared to be attempting to evade a marked Greendale Police cruiser.

50. Officer Barth asked the passenger for his identification, and he provided an Arizona identification card with the name "Estrada, Walter E.". Greendale Police Officer Christopher Houk asked for, and received consent, from Estrada to check his wallet. Upon opening the wallet, Officer Houk immediately saw a Colorado driver's license in the name of Noel Ortiz, but with a photograph of Estrada on it. The contents of the wallet also included a Bank of America credit card in the name of Noel Ortiz and two Capital One credit cards in the name of Noel Ortiz. Knowing that Estrada never identified himself as Noel Ortiz, and believing the credit cards were fraudulent, Officer Houk placed Estrada under arrest. Detective Barth contacted the Kohl's loss prevention officer. The Kohl's employee indicated that the name Noel Ortiz was on the credit cards and identification used in the fraudulent gift card purchases. On Estrada's body and in the black Nissan Altima, Greendale Police Officers found a combined total of 17 credit cards with the name "Noel Ortiz". Officers also found 41 gift cards in the vehicle. The black Nissan Altima containing Estrada and the credit cards was driven by Juan Zabala.

51. Upon review, Detective Barth confirmed Kohl's surveillance video shows Estrada purchasing gift cards on April 14 and 15, 2016 at the store using credit cards that were later confirmed to be fraudulent. On April 22, 2016, Detective Barth used a card reader to read the credit card account holders listed on the back of the cards in Estrada's possession during his arrest. The data on the back of the cards contained account numbers and names not associated with Estrada or the name Noel Ortiz. Detective Barth was able to interview eight of those victims who stated they did not give Estrada permission to possess or use their credit card information.

Elm Grove Police Department Investigation

52. On September 9, 2016, an employee at Jilly's Mobil, 15340 Bluemound Road, Elm Grove, Wisconsin, reported to Detective Craig Mayer of the Elm Grove Police Department that he

had found what appeared to be a skimmer on pump #8. The skimmer was removed with gloves and placed in evidence. Using a Mini600 version 1.3R4 software, Detective Mayer downloaded and exported the data stored on the skimmer taken from Jilly's Mobil pump #8. The results showed data for 221 victim credit card accounts.

53. On September 9, 2016, Detective Mayer reviewed the video surveillance footage for Jilly's Mobil from September 1, 2016. At 1:38 p.m. on September 1st, a red Ford Explorer drove to pump 8. The Ford Explorer was positioned in a manner whereby the opened passenger door blocked the view of the gas pump by the store employee inside Jilly's Mobil. In the video file, the driver and passenger spend a significant amount of time behind the opened passenger door and the gas pump. Seven minutes elapsed before the individuals begin pumping gas into the Ford Explorer.

54. Using his experience and knowledge that criminals may return to retrieve the skimmer on Pump #8, Detective Mayer placed a silent police radio-activation alarm on the Jilly's Mobil #8 gas pump door that same day, in an attempt to catch the individuals "red-handed" if they returned to retrieve the skimmer.

55. On September 14, 2016, at 4:13 p.m., Detective Mayer was alerted that the alarm notification system had activated and he responded to Jilly's Mobil gas station. The employee at the store stated that two men driving a red Ford Explorer had just left pump #8. The employee obtained the license plate number, DZU097.

56. A short time later, Detective Mayer was notified that Brookfield Police Officers were with the red Explorer, plate DZU097, at the Open Pantry Mobil located at 17235 Bluemound Road. The driver and passenger were identified as Richard Rivera Garcia and Josue Michel Moret. Notably, Brookfield Police had identified that another skimmer had previously been located at that

same Open Pantry on or about September 1, 2016. Rivera Garcia and Moret were taken into custody for fraud and transported to the Elm Grove P.D.

57. After the arrest, Brookfield Police Officers found a set of master keys for Open Pantry pumps hidden behind the soda machine inside of the Open Pantry Mobil store where Moret and Rivera Garcia had been arrested. Also, an improvised tool with a star-shaped bit, which could be used to open a gas pump, was found behind the candy rack. Using latex gloves and an evidence bag, Elm Grove P.D. Detective Mayer retrieved and transported the star-shaped bit tool to Jilly's Mobil pump #8 where the skimmer (later found to contain DNA from Lester Castaneda) was previously discovered. The tool was placed into the keyhole for pump #8 and did fit.

58. On September 15, 2016, Detective Mayer reviewed surveillance video from the Brookfield Open Pantry from the previous day. In the video, the red Ford Explorer was seen entering the parking lot, and the passenger, later identified as Rivera Garcia, exited the vehicle. Once inside, he could be seen throwing an object under the soda machine. Rivera also could be seen placing an object in the area where the star-shaped tool was later recovered.

59. On September 21, 2016, after their release, Elm Grove Assistant Chief Jason Hennen met with Rivera Garcia and Moret at the Police Department when they arrived to obtain their drivers licenses, credit cards and wallets. Interpreting for them was Walter Enrique Estrada. Estrada stated he was from Arizona and held an Arizona driver's license. Assistant Chief Hennen did an NCIC criminal background check and located a fraudulent use of credit card arrest on Estrada's arrest history, arrest date April 16, 2016, in Greendale, Wisconsin. Assistant Chief Hennen noted the case against Estrada was not prosecuted by the Milwaukee County District Attorney's office.

60. According to American Airline records, on September 22, 2016, Richard Rivera, Inlian Gomez, Jouse Garcia and Walter Estrada travelled together from Chicago O'Hare Airport to Miami Airport. The email address gomezsayonara@yahoo.com was used as the contact information when the flight was booked. That email address is known to be used by Inlian Sayonara Gomez. The flight was paid using Rivera Garcia's Merrick Bank credit card ending in ...3157.

Elm Grove DNA Test Investigation

61. The day the skimmer was found at Jilly's Mobile gas station, September 9, 2016, Detective Mayer used a sterile swab and made a swipe for DNA analysis from the skimmer taken from gas pump #8. On September 16, 2016, search warrants for Rivera Garcia's and Moret's DNA were signed by Waukesha County Circuit Court Judge Ramirez. The search warrants for Rivera's and Moret's cellular phones were also signed by Waukesha County Circuit Court Judge Ramirez. On September 16, 2016, Officer Townsend went to the Waukesha County Jail and collected biological specimens (DNA) from both Rivera Garcia and Moret.

62. The swab sample was sent to the Wisconsin Department of Justice State Crime Laboratory – Madison for analysis. The laboratory performed an STR DNA profile. The major STR DNA profile detected from the card skimmer swabs was entered into the FBI Combined DNA Index System (CODIS) system on November 29, 2016. On December 6, 2016, a search by the CODIS showed a match between the DNA found on the Elm Grove skimmer and the DNA for Lester Castaneda. The DNA profile for Castaneda previously matched the CODIS DNA profile found on a gas pump skimmer discovered by police in Fairview Park, OH on July 21, 2016. The Fairview Park, OH, skimmer incident was already under federal investigation at the time by your Affiant.

63. On March 14, 2018, Castaneda was interviewed by your Affiant and FBI SA Paul Cruz. Castaneda admitted to assembling gas pump skimmers. When asked how his DNA was found on a skimmer in Wisconsin, Castaneda said that in the summer of 2016, he had sold one skimmer in Miami to Nilo. Castaneda described as follows:

Two skimmers that Castaneda made were sold to Nilo. Castaneda met Nilo a long time ago in Miami, through mutual friend Ernesto Falla. Nilo called Castaneda in July or August 2016 to get skimmers. Castaneda was in Miami at the time. Castaneda met Nilo at a Shell station in Miami Lakes, near 154th Ave, Palmetto and a Cancun Grill restaurant [description matches the Shell station 15404 NW 77th Ct., Miami Lakes, FL]. Nilo showed up alone in a white BMW. Castaneda sold him the skimmers for \$2000 and Nilo said he would put the skimmers to work.

Nilo must have given the skimmers to Richard Rivera Garcia, who took it to Wisconsin. Castaneda then confirmed a driver's license photo of Nunez-Perez was the individual to whom he had sold the skimmer.

64. Through previous witness interviews and investigation, Nunez-Perez is known by your Affiant to have been a co-conspirator of Rivera Garcia. On the iPhone 6s Plus (A1687), found with Rivera Garcia during his Elm Grove investigation and arrest, is data showing 31 phone calls to and from contact "Nilo Bueno" at (305) 794-7523. Database checks show that phone number is registered to Nilo Nunez-Perez. Those 31 calls were made in the three months leading to Rivera Garcia's arrest in Wisconsin.

Clarendon County Sheriff's Department Investigation

65. On March 6, 2017, Clarendon County, South Carolina, Deputy Sheriff Ernest Grice performed a traffic stop on a vehicle for failure to use a turn signal and failure to maintain traffic lane. As Grice approached the vehicle, he noticed in plain sight inside the vehicle, new merchandise consistent with the occupants returning from a shopping trip. Grice spoke to the driver, Cesar Lopez, who appeared to be nervous. The passenger, Alfonso Gouirrie-Blanco also appeared nervous to Grice. Lopez told Grice he was returning from visiting friends and going to bars in New Jersey. Grice asked Lopez if that was all they had done on the trip, and Lopez said "yes." Lopez also told Grice he was unemployed. Grice thought that seemed odd because of all the new merchandise in the vehicle. Neither Gouirrie-Blanco nor Lopez were listed on the vehicle rental agreement as an authorized driver, and the agreement showed that the vehicle was overdue to be returned by two days.

66. Deputy Grice asked Lopez for consent to search the vehicle and Lopez granted consent. During the consent search, a Dell Inspiron 15 model laptop computer was found. Also inside the bag containing the laptop was an American Express card in the name of Marco Ricci. Grice and Deputy Bandon Braxton knew from their training and experience that the card was counterfeit. Gouirrie-Blanco and Lopez were detained, and the vehicle was further searched. Secreted behind the passenger side interior panel were two bags containing what the deputies knew from their training and experience to be gas pump skimmers and a credit card reader used to take credit card information from a gas pump or ATM. Under the interior carpet on the driver's side of the vehicle were secreted plastic bags with additional skimmers and a wallet with several additional counterfeit credit cards. Near the passenger seat a stack of credit cards in a rubber band was located. Also found were two pages of what appeared to be handwritten bank account

numbers and/or pass codes. Lopez and Gouirre-Blanco were placed under arrest and transported to Clarendon County Jail. Nine skimming devices were found in the vehicle.

67. Also found in the vehicle was media CD-R DVD-R labeled in black marker, "Elm Grove PD Cases 16-469 & 16-474, gas pump skimmer video from Mobil of gas pump skimmer video from September 1, 2016, video from Mobil of gas pump skimmer, Def. Josue M. Garcia Moret, Def Richard Rivera-Garcia." Clarendon County Sheriff Deputies called Elm Grove P.D. Detective Mayer, who stated the CD-R was part of the trial discovery items given to Rivera Garcia's attorneys in preparation for his potential trial in Wisconsin. Detective Mayer then notified your Affiant. Your Affiant spoke to Dep. Braxton by phone and informed him that Rivera Garcia was the head of a multi-state travelling organization connected by DNA to skimmers found in Ohio and Wisconsin. Dep. Braxton agreed to transfer the evidence found in the vehicle to the Cleveland, Ohio U.S. Secret Service Office.

Rental Information for Clarendon County Vehicle Stop

68. On March 9, 2017, your Affiant contacted Dollar Rental Car / Hertz Law Enforcement Representative Sam Milanovich, regarding the 2016 Nissan Quest driven by Blanco and Lopez at the time of their arrested in Clarendon County, SC. The vehicle was rented out of the Miami FL Airport on February 22, 2016, by Sergio Rivera. Sergio Rivera's Florida drivers' license R160780630920, date of birth March 12, 1963, address 14682 SW 143rd Terrace, Miami, was used to rent the vehicle.

69. The individual who rented the vehicle has the same name, address and date of birth as Richard Rivera Garcia's father, Sergio Rivera. The address, 14682 SW 143rd Terrace, Miami, was also used on a previous Florida Driver's License for Richard Rivera Garcia.. Also of note, the iPhone 7 (A1661) found in the possession of Rivera Garcia during his federal arrest on July 6,

2017 showed three phone connections were made from Rivera Garcia (305) 915-7228 to Alfredo Gouirrie-Blanco (201) 280-5622 on March 24, 2017. This was the phone number listed for Gouirrie-Blanco in Kenner, Louisiana, Police Department records from Gouirrie-Blanco's arrest on December 4, 2017.

Kenner Police Department Investigation

70. On December 1, 2017, at the Discount Zone gas station, 4045 Williams Blvd., Kenner, Louisiana, employees received a number of credit card charge-backs. Charge-backs are sometimes an indication that someone may have placed a skimmer on a gas pump internal payment computer. A gas station employee opened the pumps and discovered skimmers on pump 4 and pump 6.

71. Later that day, a station employee noted the gas pump audio notification sounded inside of the store, signaling a nozzle was removed from a pump by a customer. However, he did not receive the follow-up notification which had indicated the pump had begun to dispense fuel. The employee looked at pump 4 to determine why the nozzle was removed, but no gas was pumped. The employee saw two subjects that appeared to be hiding behind the pump, and one of them had the pump access door open. The access door has a lock that is kept closed and the door is normally locked and secured shut. A third individual was in the store and attempted to distract the employee. When the employee saw the pump door was opened, the employee came around the counter and took a photo of the vehicle with his phone. The photograph included the vehicle's license plate. The individuals at the pump closed the pump door and all three fled the station in a maroon Dodge Caravan with Mississippi plate LVP617.

72. On December 4, 2017, Kenner Police Officers located that vehicle travelling westbound on Veterans Blvd. and conducted a vehicle stop. Sandy Alvarez was driving, Alfredo

Gouirrie-Blanco was in the passenger seat and Yunior Rodriguez was in the mid-row passenger seat. The three were transported to the Kenner Police Department. At the intake counter, Detective Brad Ricke observed two keys in Gouirrie-Blanco's property. The keys were later found to be compatible with the Discount Zone gas pump locks.

73. Pursuant to a search warrant, on December 5, 2017, Kenner detectives conducted a search of the maroon Dodge Caravan with Mississippi plate LVP617. Using a credit card reader, Detective Ricke found that eight credit cards located in the vehicle had different account data on the magnetic strip than the account numbers written on the fronts of the cards, indicating the credit cards were counterfeit.

74. Notably, the location where Gouirrie Blanco was arrested in Kenner, Louisiana, is less than a half mile from the address of Richard Rivera Garcia's grandfather, Sergio Garcia Sr. Bank records, American Airline records and witness statements indicate that Richard Rivera Garcia began the 2016 skimming and credit card scheme in Kenner, LA on or about July 13, 2016 to on or about August 3, 2016, prior to departing for Oklahoma City and Milwaukee. The address of Sergio Garcia Sr., 4315 Florida Ave. Apt D, was sent in a message dated July 14, 2016 in Moret's Samsung Galaxy S6 cell phone seized in Elm Grove. That address was also in a message dated August 15, 2016, from Rivera Garcia's iPhone 6s Plus (A1687) seized in Elm Grove. Western Union records show that Sergio Rivera Sr. used this address when he made wires overseas. Database searches also show this address as a residence of Sergio Rivera Sr. at the time of Gouirrie-Blanco's arrest in Kenner.

Forensic Exams of Cellular Telephones and Electronic Devices Used As Evidence

75. On September 22, 2016, Detective Brad Warhanek of the City of Brookfield, Wisconsin, Police Department completed a Cellebrite Extraction Report for the data that was

found on the Apple iPhone 6s Plus (A1687) which was found in the possession of Rivera Garcia during his arrest by Elm Grove police. In the phone's data files were numerous photos of gas station map locations across Oklahoma, Illinois and Wisconsin, including the Open Pantry Mobil located at 17235 Bluemound Road. In the GPS section of the Extraction Report are geographic locations which indicate the iPhone 6s Plus (A1687) had traveled from Oklahoma City to the Milwaukee area between August 29, 2016 to September 14, 2016. Additionally, in the iPhone 6s Plus (A1687) from Elm Grove, there were numerous photos of U.S. Postal Service Priority Mail slips, stacks of gift cards and images handwritten notes of retailer names and dollar amounts for gift cards. Many of these text message photos were sent to or came from (786) 554-9368. This is the phone number for Rivera Garcia's girlfriend, Inlian Sayonara Gomez. The GPS location on many of the gift card photos sent from Gomez correspond to her apartment location, 15272 SW 104th St., Miami, Florida.

76. One photo found in a text message, dated August 17, 2016 in the iPhone 6s Plus (A1687), found in the possession of Rivera Garcia during his arrest by Elm Grove showed the full account numbers on the backs of twelve Walmart gift cards. On September 19, 2017, Walmart Global Investigator Michael Wisely completed a report tracing the payment source for the twelve Walmart cards. None of the payment credit card numbers used to buy the Walmart gift cards corresponded to known accounts for Rivera Garcia or his co-conspirators. The Walmart gift cards were activated and used at Walmart stores in the Oklahoma City area during the time period when Rivera Garcia and his associates were known to have stayed in the area.

77. This same photo of twelve Walmart gift cards from Oklahoma City was later found in the data files in the image files of the Dell Inspiron 15 laptop computer that was in the vehicle with Rivera Garcia's co-conspirators Alfredo Gouirrie-Blanco and Cesar Lopez during their arrest

in Clarendon County, South Carolina on March 6, 2017. In addition, this computer contained 21 image files that were also found in Rivera Garcia's iPhone 6s Plus (A1687) seized in Elm Grove. Pursuant to a search warrant, between June 23, 2017 and July 25, 2017, USSS SA Ronald Koelsch performed a forensic exam on the Dell Inspiron 15 laptop computer that was in the vehicle with Gouirrie-Blanco and Lopez during their arrest in Clarendon County, SC. 136 credit card account numbers were found on the data files of the computer. A file named "ale" contained credit card numbers and the email address ale_moro2005@yahoo.es was found as a log in address for the web site Joker's Stash. Joker's Stash is a known dark web "carding" site, where victims' credit card numbers are bought and sold. USSS investigation has shown Rivera co-conspirator Alejandro Rodriguez Martinez has the nicknames "Ale" and "Moro".

78. The network system information showed Wi-Fi networks that the computer had logged into. Among these log-in locations were several that corresponded with known locations where Richard Rivera and his co-conspirators were suspected of committing crimes involving gas pump skimmers and use of counterfeit credit cards. These locations included a network named LaQuinta, with a first connection time of August 7, 2016, and a last connection time of September 1, 2016. This time period corresponds with Rivera Garcia's iPhone 6s Plus (A1687) GPS location of 4829 Northwest Expressway, Oklahoma City, OK. Public records indicate this address is the LaQuinta Inn & Suites Oklahoma City. Ocean Bank records and LaQuinta Inn lodging records show that Rivera Garcia's co-conspirator Frank Bernal had rented a room at the LaQuinta from August 8, 2016 to August 9, 2016 and from August 16 to August 30, 2016.

79. On November 9, 2017, an additional forensic examination was performed on the Dell Inspiron 15 laptop computer that was in the vehicle with Gouirrie-Blanco and Lopez during their arrest in Clarendon County, SC. 136 credit card account numbers with other individuals'

names were found in files on the computer. In the computer image files were at least twenty of the same photographs found in the data files of the iPhone 6s Plus (A1687) seized from Rivera Garcia during his arrest in Elm Grove. The photos were of gift cards, shipping labels and the handwritten bookkeeping from Inlian S. Gomez. The photo and message timestamps corresponded to the times of Rivera Garcia's skimming and shopping activities in Milwaukee, Oklahoma City and Chicago.

80. On July 27, 2017, pursuant to a search warrant, USSS SA Ian McIntyre completed a Cellebrite Extraction Report for the Apple iPhone 5s (A1533) found with Alfredo Gouirrie-Blanco during his arrest in Clarendon County, SC. In the cell phone call logs were 72 calls between Gouirrie-Blanco and "Richar" (305) 591-7228 between August 9, 2016 and March 4, 2017. The phone registered to that number (305) 591-7228 was found on Richard Rivera Garcia's person when he was arrested by the USSS on July 6, 2017. USSS SA Ian McIntyre also performed a forensic data examination on the nine skimming devices found in Gouirrie-Blanco's vehicle by Clarendon County, SC Sheriff's deputies. The chips were connected to a Dataman-48 Pro+ Universal Programmer. In the binary files for the nine skimmers found in the vehicle with Gouirrie-Blanco were the names and account numbers for 2,996 credit card customers.

Rivera Garcia Federal Arrest, Hialeah, Florida

81. On June 28, 2017, a federal indictment for Rivera Garcia related to violations of 18 U.S.C. §§ 1029(a)(2)(Access Device Fraud), 1029(a)(3) (Possession of 15 or more counterfeit or unauthorized Access Devices); and 1028A(a)(3) (Aggravated ID Theft) was obtained in the Northern District of Ohio. Among the four other suspects named in the indictment was Lester Castaneda, the individual whose DNA was found on skimmer found at the at Jilly's Mobil, 15340

Bluemound Road, Elm Grove, Wisconsin on September 9, 2016. Castaneda's DNA had also been found on a skimmer found in a gas station pump in Fairview Park, Ohio, on or about July 21, 2016.

82. On July 6, 2017, agents of the USSS and U.S. Marshals Service located Rivera Garcia at a residence located at 7430 N Augusta Drive, Hialeah, Florida. During this arrest, ten counterfeit access device cards were found in Rivera Garcia's possession. Each counterfeit credit card was encoded with ten names that were not Rivera Garcia and the names did not correspond to the cardholder and/or gift card names printed on the cards.

83. In Affiant's training and experience, organizations committing credit card fraud and placing gas pump skimmers travel extensively in order to attempt to confuse authorities, hide their activities and compartmentalize arrested individuals to prevent them from compromising the organization. Planners of the criminal activity send subordinates in the organization to great distances to evade investigation and prosecution. Due to manpower and extradition limits for local law enforcement entities, criminals know that even after arrest, local authorities cannot travel to investigate and apprehend them.

84. Investigation to date has revealed that Richard Rivera Garcia is the leader of such a traveling organization, responsible for multiple crimes occurring in, but not limited to, Ohio, Wisconsin, Florida and South Carolina. The items described in this narrative are evidence of this activity.

Email Nexus to the Conspiracy

85. Review of subpoenaed documents and forensic reports show the following Yahoo! and Google email accounts were used by the co-conspirators during the course of the events described above.

- a. richardela@yahoo.com was the registration Apple ID for iPhone 6s Plus (A1687) seized by Elm Grove PD from Rivera Garcia on September 14, 2016
- b. riveragarcia0610@gmail.com was the registration Apple ID for iPhone 7 Plus (A1661) seized by USSS SAs from Rivera Garcia in Miami on July 6, 2017
- c. maktub631@yahoo.com was used as the contact information by Walter Estrada for his Arizona Federal Credit Union account
- d. gomezsayo@yahoo.com was found in the Recently Contacted file in the iPhone 6s Plus (A1687) seized by Elm Grove PD from Rivera Garcia. This email address is also listed as a contact for Inlian Gomez in her Barclaycard account application 61305832 dated April 20, 2017
- e. gomezsayonara@yahoo.com was listed on Inlian Gomez in her Barclaycard account application 37388913 dated March 31, 2014. This email address was also used as the contact to purchase American Airline flights for Richard Rivera Garcia, Josue Michel Moret, Juan Zabala and Walter Estrada
- f. josuegarcia1990@yahoo.com used as the contact to purchase an American Airlines flight for Moret and Rivera Garcia
- g. rivera.sergio32@yahoo.com was used as the contact to purchase an American Airlines flight for Rivera Garcia
- h. yetsycubana@yahoo.es was used to book American Airlines flights for Juan Zabala
- i. frankabel28@yahoo.com was used on co-conspirator Frank Bernal on the Ocean Bank account used to book a room at the LaQuinta hotel in Oklahoma City in August 2016

- j. megacesar2@gmail.com was the registration Apple ID for iPhone 6 (A1549) seized from the vehicle of Cesar Lopez during his arrest in Clarendon County, SC
- k. garciadirian@yahoo.com was used to book American Airline flights for Rivera Garcia, Juan Zabala, Walter Estrada
- l. ale_moro2005@yahoo.com was found in an August 5, 2016 text message iPhone 6s Plus (A1687) seized by Elm Grove PD from Rivera Garcia
- m. ale_moro2005@yahoo.es was found during a forensic exam of the computer found with Gouirrie-Blanco in Clarendon County. Data files show ale_moro2005.es as a log in address for the web site Joker's Stash. Joker's Stash is a known dark web "carding" site, where victims' credit card numbers are uploaded, bought and sold
- n. yunitica@gmail.com was the Apple ID for iPhone 5s (A1533) seized from the vehicle of Gouirrie-Blanco during his arrest in Clarendon County, SC
- o. alfeditogouirrie@gmail.com was the address found in emails from the iPhone 5s (A1533) seized from the vehicle of Gouirrie-Blanco during his arrest in Clarendon County, SC

86. This Affiant believes the Google, Inc. and Yahoo! email-related data, including the historical geo-location data (GPS) may be important in establishing locations and activities of possible witnesses, victims, co-conspirators, and suspects. This information may also be important in establishing the driver and occupants of a particular vehicle, refute and corroborate statements, and can be used to establish a timeline and provide context and intent.

87. For the reasons outlined above, this Affiant believes probable cause exists to seize and examine the specified records held by Google, Inc. and Yahoo! accounts named herein. The records to be searched for and seized are more particularly described as Attachment A – Yahoo!

Items to be Seized and Attachment B - Google, Inc Items to be Seized.

Telephone Nexus to the Conspiracy

88. Review of subpoenaed documents and forensic reports show the following telephone accounts were used by the co-conspirators during the course of the events described above.

- a. Richard Rivera Garcia, phone 786-878-2960, 786-351-7385, 305-915-7228, phone numbers 786-878-2960, 786-351-7385 for phones found in Moret and Rivera Garcia's possession during their arrests in Elm Grove, Wisconsin in 2016; phone number 305-915-7228 for the phone found in Rivera Garcia's possession during his arrest in Hialeah, Florida in 2017
- b. Josue Michel Garcia Moret, phone 956-510-2392; 324 calls from Rivera Garcia from 7/12/16 to 9/14/16
- c. Sergio Rivera, phone 305-253-2037; Vehicle driven by Alfredo Gouirrie-Blanco during his arrest in Clarendon County, South Carolina was a rental for 2016 Nissan Quest, rented at the Miami Airport on 2/22/17 by Sergio Rivera, phone number 305-253-2037
- d. Inlian Sayonara Gomez, phone 786-554-9368, 786-857-1600, 786-560-6860, 786-720-6251; 148 outgoing calls to 786-554-9368 and 786-720-6251 from Rivera Garcia from 7/12/16 to 9/14/16; 71 outgoing calls to 786-857-1600 and 786-560-6860 from Rivera Garcia between 11/23/16 and 7/7/17
- e. Cesar David Lopez, phone 786-972-6898; 20 outgoing calls from Gouirrie-Blanco from 8/9/16 to 3/4/17
- f. Gabriel Delgado Ramirez, phone 305-988-3292; 274 calls from Rivera

Garcia from 7/12/16 to 9/14/16

g. Frank Abel Bernal, phone 786-506-0292; 95 274 calls from Rivera Garcia from 7/12/16 to 9/14/16

h. Alfredo Gouirrie-Blanco, phone 201-280-5622, 305-699-8792; phone number 305-699-8792 was the phone found in Gouirrie-Blanco's possession during his arrest in Clarendon County, South Carolina; the iPhone found in the possession of Rivera Garcia during his federal arrest on July 6, 2017 showed three phone connections were made from Rivera Garcia to Alfredo Gouirrie-Blanco (201)280-5622 on March 24, 2017. This was also the phone number listed for Gouirrie-Blanco in Kenner, Louisiana, Police Department records from Gouirrie-Blanco's arrest on December 4, 2017.

i. Walter Enrique Estrada, phone 623-216-8599, 623-707-9147; 124 calls from Rivera Garcia from 7/12/16 to 9/14/16; phone number 623-707-9147 was on court summons from Estrada's arrest in Greendale, Wisconsin

j. Nilo Nunez-Perez, phone 305-794-7523; 31 phone calls to and from Rivera Garcia to Nunez-Perez from 7/12/16 to 9/14/16.

k. Alejandro Rodriguez Martinez, phone 305-587-6005; 224 calls from Rivera Garcia from 7/12/16 to 9/14/16

l. Jose Javier Moreiras, phone 786-856-7039, 786-878-0825; 312 calls to these phone numbers from Rivera Garcia from 7/12/16 to 9/14/16

Authorization for Electronic Service

89. This Affiant also requests authorization to execute the search warrant for the requested records via electronic means including facsimile or other electronic transmission in

accordance with ORS 136.583.

CONCLUSION

90. Based on the foregoing information, this Affiant has probable cause to believe that within the Target Email Accounts and Target Phone Accounts described above there exists fruits, evidence or instrumentalities of the violations of Title 18, United States Code, Sections 1029(a)(2), 1029(a)3 and 1028A(a)(1), as set forth herein are currently within the records described above. This Affiant therefore respectfully requests that a search warrant be issued authorizing the search for, seizure of and examination of the records set forth in herein.